# Internet y Redes sociales: Acoso y otros riesgos

**Título:** Internet y Redes sociales: Acoso y otros riesgos. **Target:** ESO y Bachillerato. **Asignatura:** Todas. **Autor:** José Manuel Muñoz Simó, Ingeniero Técnico en Informática de Gestión, Desarrollador Software en Docler Holding (Luxemburgo).

Las Redes Sociales se han convertido en un hervidero de problemas. No solo niños sino también adultos suben fotos a internet, comentan su día a día, conocen gente nueva y mucho más de forma incontrolada. ¿Pero nos podemos fiar? Evidentemente no.

Palpablemente, no solo en internet está el peligro sino también en la calle. La diferencia es que en internet a menudo se tiene una falsa sensación de seguridad. Se debe de tener en cuenta que todo aquello que se publica en las redes sociales, de una forma u otra puede llegar a ser público, ya sea por carecer de conocimiento, por falta de formación o por exceso de confianza, y todo esto se puede volver en nuestra contra.

¿Sabemos a lo que nos exponemos? ¿Sabemos cómo protegernos? ¿Sabemos cómo orientar a nuestros alumnos para que no se expongan a riesgos? En este artículo se analizará eso y mucho más.

## DELITOS MÁS COMUNES EN LAS REDES SOCIALES E INTERNET

A día de hoy, las redes sociales son otro medio por el que se cometen delitos: amenazas, usurpación de identidad, publicación de información privada, phishing, acoso, calumnias, grooming y ciberbullying son los más comunes.

Para conocer los peligros es necesario entenderlos, e igualmente se puede ver cómo el código penal se toma muy enserio este tipo de delitos:

- **Amenazas**: Según la RAE, amenazar es dar a entender con actos o palabras que se quiere hacer algún mal a alguien. Es bastante común, sobre todo en los jóvenes, recibir amenazas mediante el uso de redes sociales, con la intención de causar miedo o inquietos a la persona receptora.

  Cuando estas amenazas son anónimas, la víctima puede pensar que es complicado averiguar quien realizó dicha amenaza. Sin embargo, es bastante sencillo poder identificar al autor con los actuales medios técnicos, lo cual está ocasionando una tendencia positiva en la denuncia de éstos.

  En el código penal se indica que según el tipo de amenaza y la gravedad de ésta, puede conducir a una multa y/o penas de prisión de entre 3 meses a 5 años (TÍTULO VI - Delitos contra la libertad, CAPÍTULO II - De las amenazas, Artículos 169, 170 y 171).

- **Acoso**: Hay diversas formas de recibir acoso. Algunos ejemplos de acoso por internet incluyen mensajes desagradables (vía email, redes sociales u otros), rumores publicados en sitios de redes sociales, imágenes, videos, sitios web o perfiles falsos embarazosos. Una derivación del acoso es el **cyberbullying** y **grooming**. En algunos casos incluyen **amenazas** (explicado en el punto anterior), **calumnias** y **publicación de información privada**.

- **Cyberbullying** (ciberacoso escolar): Se refiere al acoso entre menores online. Es frecuente que el acoso online sea acompañado por acoso también en persona. Es con diferencia el caso más común.

- **Grooming**: Ocurre cuando un adulto pretende ganarse la amistad de un menor con el fin de poder aprovecharse o abusar sexualmente de él. En casos extremos, podría llegarse al punto de introducir a la víctima en el mundo de la prostitución infantil y/o la producción de pornografía infantil.

Este tipo de jóvenes a menudo termina estando inmerso en otros problemas, como el consumo de drogas o alcohol, problemas de autoestima, abandono escolar, etc.

El código penal hace referencia al acoso en el TÍTULO VIII - Delitos contra la libertad e indemnidad sexuales, en el que explica las diversas formas de acoso que son castigadas y penadas, llegando en algunos casos a alcanzar penas de prisión de hasta 12 o 15 años.

- **Usurpación de identidad** (robo de identidad): Consiste en hacerse pasar por otra persona para así en acceder a ciertos recursos u obtener otros beneficios en nombre de esa persona.

Por otro lado, el robo de identidad también es utilizado con el fin de perjudicar a una persona y no solo el de beneficiarse de ésta. Para ello, simplemente puede crear un perfil en una red social con el nombre de la víctima y añadir algunas fotos suyas.

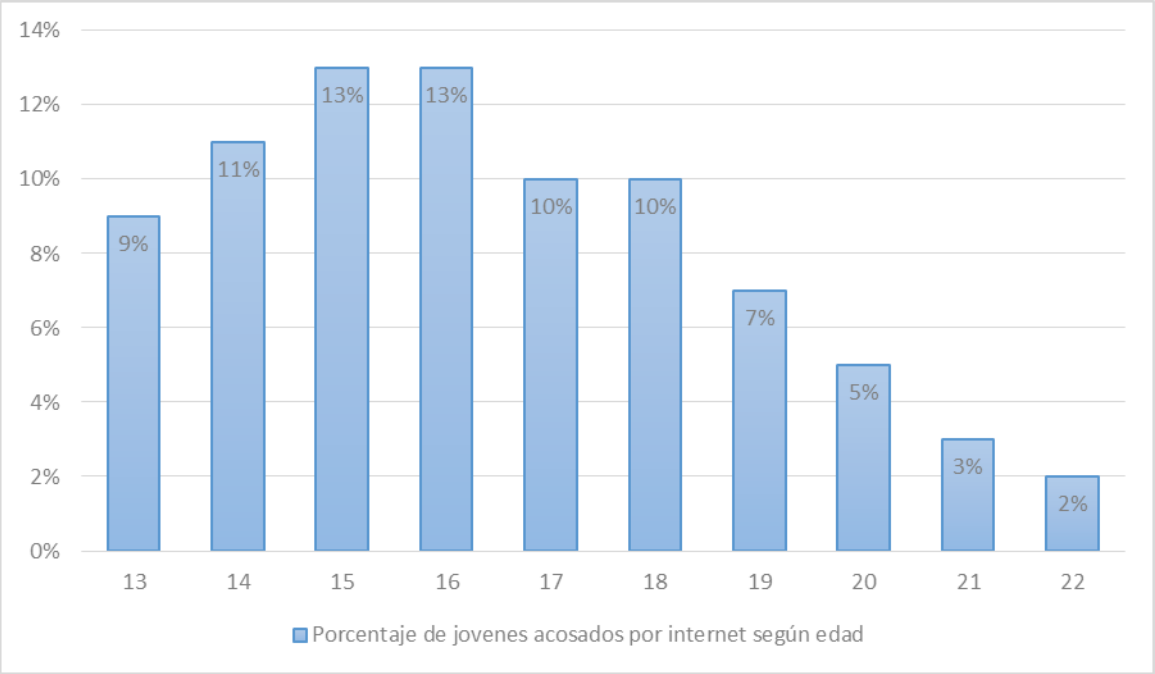
En el código penal se indica que "*El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años*" (TÍTULO XVIII - De las falsedades, CAPÍTULO IV - De la usurpación del estado civil, Artículo 401).

- **Phisihing**: Son enlaces que llevan a páginas webs falsificadas con el fin de hacer creer al usuario que están en un sitio de toda confianza, en donde introducen la información que se solicita y que en realidad, va a parar a manos de estafador. Este riesgo no está solo en las redes sociales, sino en todo internet realmente.

Ya sea en un grupo dentro de una red social, o a través de algún contacto, un email conocido o desconocido, o desde otra fuente, podemos encontrarnos con un enlace de estas características, cuyas consecuencias pueden ser no solo la pérdida de información confidencial, sino el que el estafador pueda bloquear el acceso a dichos sitios.

En el código penal se indica que según el tipo de fraude (el cual incluye el fraude informático) y la gravedad de éste, puede conducir a penas de prisión de entre 3 meses a 6 años (TÍTULO XIII - Delitos contra el patrimonio y contra el orden socioeconómico, CAPÍTULO VI - De las defraudaciones, SECCIÓN 1 - De las estafas, Artículos 248, 249, 250 y 250 bis).

Y es que la recurrencia de este tipo de delitos se superan año tras año, y el acoso por internet se está convirtiendo en un problema cada día más presente. Algunos datos estadísticos mundiales representados en el anuario de ciberbullying de 2013 de DitchTheLabel.com son los siguientes:




**PREVENIR RIESGOS EN LAS REDES SOCIALES E INTERNET**

No solo adultos sino los niños deben de concienciarse de los peligros. Para evitar correr riesgos, mejor actuar de forma preventiva:

1. **No publiques información comprometida**. Ni en Twitter ni en Facebook, o similares, no proporciones datos que permitan a otros ubicar tu domicilio, escuela, lugar de trabajo, etc. Todo lo que escribas en Twitter es público, por lo que tener una cuenta privada y contar tus detalles íntimos no es muy recomendable. Facebook es configurable, y se debe de tener en cuenta que según como lo configures, habrá más gente o menos que tenga acceso a más o menos cosas de las que publiques.

2. **Configura los parámetros de privacidad**: Todas las redes sociales incorporan opciones de privacidad para configurarlas a tu gusto. Tú decides quién accede a tus contenidos y cómo. Revísalas bien antes de publicar nada. Es preferible organizar a tus contactos por listas o categorías y ofrecerles contenidos con distintos niveles de privacidad. En Facebook, por ejemplo, una opción recomendable es filtrar quién puede leer y publicar en tu muro.

3. **Supervisa la actividad a alumnos y otros menores de edad en la red:** Seas profesor, familiar o amigo, la supervisión de las actividades de los menores en la red es importante, pero no es lo único que se debe de hacer. Igual que enseñamos a los jóvenes a comportarse y actuar en el entorno que les rodea, debemos de darle a conocer los riesgos de internet. Como comentan en abcblogs.abc.es [12]: *Es mejor un niño ilustrado y con autonomía que uno vigilado ignorante*.

4. **No aceptes relaciones con desconocidos**: Aprende a diferenciar los matices del concepto de "seguidor" y "amigo" en la red. En Facebook solo deberías agregar a personas que conozcas y que te inspiren

confianza, ya que ahí pueden tener acceso a fotos más comprometidas o comentarios personales. Los menores de edad podrían dejarse convencer mediante el engaño y establecer relación con personas que no son quien dicen ser. Si eres una víctima o conoces a alguien que lo esté siendo, debes contárselo a padres, tutores o profesores, y actuar al respecto.

5. **No te inscribas en foros radicales** o de cualquier temática en la que sabes que si participas pueden ir en contra de ti. Si lo haces, se consciente de las posibles consecuencias, y cuida de que no puedan averiguar ninguna información personal a través de tu perfil en el foro para evitar el acoso.

6. **No te fíes de cualquier página**: Hay muchos sitios que no son seguros y pueden utilizar tus datos de forma ilícita, o en su defecto pueden facilitar a hackers obtener ciertos datos confidenciales. Limítate a dar tus datos sólo a las webs que sepas que son de plena confianza. Si estás usando datos confidenciales como la tarjeta de crédito, asegúrate que la web está bajo una conexión segura (lo sabrás si ves que la dirección web empieza por https:// y tiene un candado junto al texto).

7. **No uses contraseñas sencillas**: Las contraseñas no deben de contener datos personales como fechas o nombres, y deben de ser cambiadas cada cierto tiempo. Se recomienda que las contraseñas usen letras en mayúscula y minúscula, caracteres especiales como guiones, puntos y otros símbolos, y números (todos en una sola contraseña y al menos 8 caracteres).

8. **No abras ningún archivo del que tengas dudas**: Aunque provengan de amigos y conocidos, ellos pueden haber sido infectados por malware que estén distribuyendo el mismo virus. Un sencillo ejemplo fue el virus ILoveYou, el cual hizo estragos en el año 2000. Los usuarios de internet recibían un email con el asunto ILOVEYOU y con un archivo llamado 'LOVE-LETTER-FOR-YOU. TXT.vbs', que tras abrirlo se ejecutaba en el sistema, replicándose y enviándose por correo electrónico a todos los contactos. Fácil caer, ¿no?

9. **Ten el antivirus actualizado**: Utiliza un antivirus (los hay gratuitos y buenos) y actualízalo periódicamente. No se recomienda tener más de un antivirus instalado, ya que pueden provocar que el sistema operativo se colapse y vaya mucho más lento.

10. **Usa algún programa anti-spyware**: Te eliminará muchas pistas que utilizan diferentes compañías para espiar nuestros hábitos de navegación y comportamiento, además de otras variantes de malware. Es un complemento a un antivirus, y de hecho hay antivirus que incluyen anti-spyware. Popups y páginas que se abren automáticamente son síntomas que tenemos spyware o malware.

11. **Cuidado con las redes inalámbricas**: Con los debidos conocimientos, se puede espiar lo que los demás hacen cuando éstos están conectados a redes inalámbricas. Es lo que se denomina “esnifar” los datos de la red. Expertos pueden obtener conversaciones completas e incluso contraseñas si las webs no se conectan de forma segura a la red.

12. **Cuidado con el uso de ordenadores públicos**: Si utilizas un ordenador en un centro escolar o en cualquier sitio público, asegúrate que cierras todas tus sesiones, ya que no solo basta con cerrar la ventana del navegador. Si no lo haces, otro usuario que utilice ese ordenador podría accidentalmente (o a caso hecho) acceder a tu perfil de Facebook, de cuentas de correo, etc., y así poder acceder a tu información privada o publicar cosas en tu nombre. Igualmente, asegúrate que no hay programas espía, y borra los logs de navegación si los consideras confidenciales.

Por su parte, **Panda Security**, ofrece una serie de consejos para evitar el riesgo a sufrir un problema con el **phishing (**URL: http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/):

- *Verifique la fuente de información. No conteste automáticamente a ningún correo que solicite información personal o financiera.*
- *Escriba la dirección en su navegador de internet en lugar de hacer clic en el enlace proporcionado en el correo electrónico.*
- *Compruebe que la página web en la que ha entrado es una dirección segura. Para ello, ha de empezar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado de nuestro navegador.*
- *Revise periódicamente sus cuentas para detectar transferencias o transacciones irregulares.*
- *No olvide que las entidades bancarias no solicitan información confidencial a través de canales no seguros, como el correo electrónico.*

**CÓMO EDUCAR A LOS JÓVENES ANTE ESTOS PELIGROS**

Si bien es cierto que las redes sociales están trabajando para evitar abusos y estafas, siguen éstas siendo peligrosas para aquel que no conoce sus peligros. Se tiene que tener en cuenta que hay personas que pueden acceder a los jóvenes y no tan jóvenes, y por eso, lo mejor es educar y enseñarles algunas precauciones necesarias para tales casos.

Por ejemplo, debemos explicarles de los peligros de chatear o hablar con desconocidos, y que no deben de confiar en nadie si no están seguros al 100%, ya que cualquier persona puede poner la foto de una persona y hacerse pasar por él. También, si dado el momento el menor quiere conocer a alguien, la mejor idea será acompañarlo, ya sea alguno de sus padres, o un hermano mayor u otro pariente que pueda reaccionar en caso de necesidad.

Otro consejo elemental es insistirles en no publicar información personal, tal como dirección, número de teléfono, o incluso sus actividades y horarios. De igual modo, los adultos no deben publicar información como la descrita, ni los datos de su estado bancario, cuentas, tarjetas u otras a desconocidos. Se recomienda no colgar fotos de los menores en la red en espacios públicos como un blog o similar, ya que pedófilos u otros sujetos desagradables pueden dar con ellos.

**DENUNCIAR ONLINE**

Aun evitando situaciones de acoso, hay veces en los que se cae en este problema. Para ello, diversas redes sociales tienen enlaces donde denunciar estos problemas, además de una serie de consejos e indicaciones para proceder a realizar dichas denuncias. Para eliminar imágenes o comentarios inapropiados, es sin duda la mejor opción.

Algunos de los enlaces de las principales redes sociales utilizadas en España son:

- Facebook: https://www.facebook.com/note.php?note_id=212294155454750
- Tuenti: http://corporate.tuenti.com/es/help/police/es

- Badoo: https://badoo.com/es/help/?section=89
- Yahoo: https://es.ayuda.yahoo.com/kb/messenger/Notificar-un-abuso-en-Yahoo-Messenger-sln494.html
- Twitter: https://support.twitter.com/forms/abusiveuser
- Google (incluye Google+, YouTube y Blogger): https://www.google.com/intl/es-419/goodtoknow/familysafety/abuse/

**SI ES NECESARIO, ACTÚA**

Evidentemente, si cualquier caso aparece y se nos escapa de las manos, deberemos de acudir a la Policía Nacional. Desde la Oficina Virtual de Denuncias de la Policía Nacional (https://denuncias.policia.es/OVD) pueden ayudarnos, pero en caso que la víctima de abusos por internet sea menor de edad, se deberá acudir "in situ".

Nunca se debe de ceder a amenazas o chantajes, tienes que denunciar inmediatamente. Muchos de los acosadores creen que son impunes por encontrarse detrás de un ordenador, y es probable que se lleven una desagradable sorpresa al ver que los delitos que hacen de forma anónima por internet están penalizados y son fácilmente perseguibles y denunciables ante la policía o un juez.

Si te están acosando, denúncialo a la policía de tu país, y por supuesto, aportando pruebas: conversaciones en un chat, capturas de pantalla, tu propio perfil en un foro en el que te amenazan, etc. Todo sirve.

Cuando las autoridades competentes revisen el caso, si ven que efectivamente existe acoso, amenazas, estafas o cualquier otro delito, citarán a un juicio rápido al acusado, normalmente sin la intervención del afectado, ya que la acusación la llevará a cabo un fiscal de oficio.

**CONCLUSIÓN**

Internet y las redes sociales nos ofrecen grandísimas ventajas, aunque inevitablemente acompañan otros problemas. En este artículo se dan algunos consejos e información relevante para prevenir y actuar ante posibles problemas que puedan surgir.

**Bibliografía**

[1]. "Base de Datos de Legislación, TÍTULO VI - Delitos contra la libertad", Noticias Jurídicas.
URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t6.html

[2]. "Base de Datos de Legislación, TÍTULO VIII - Delitos contra la libertad e indemnidad sexuales", Noticias Jurídicas.
URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t8.html

[3]. "Base de Datos de Legislación, TÍTULO XIII - Delitos contra el patrimonio y contra el orden socioeconómico ", Noticias Jurídicas.
URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html

[4]. "Base de Datos de Legislación, TÍTULO XVIII - De las falsedades", Noticias Jurídicas.

URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t18.html

[5]. "Me han amenazado en las redes", Teva Mont Advocats.
URL: http://www.tevamontadvocats.es/amenazado-amenazar-amenazas/

[6]. "¿Qué es el acoso por internet?", StopBulling.
URL: http://espanol.stopbullying.gov/acoso-por-internet/qué-es/ur6/índice.html

[7]. "¿Es delito suplantar la identidad de otro?", PabloBurgueno.com.
URL: http://www.pabloburgueno.com/2010/03/%C2%BFes-delito-suplantar-la-identidad-de-otro/

[8]. "Phishing", Panda Security.
URL: http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

[9]. "Cyberbullying and Bullying Statistics 2014, Finally", NoBulling.
URL: http://nobullying.com/cyberbullying-bullying-statistics-2014-finally/

[10]. "Cómo Evitar el Acoso en Internet", ComoHacerPara.
URL: http://comohacerpara.com/como-evitar-el-acoso-en-internet_7077s.html

[11]. "ILoveYou", Wikipedia.
URL: https://es.wikipedia.org/wiki/ILoveYou

[12]. "8 recomendaciones para evitar correr riesgos en redes sociales", ABC.
URL: http://abcblogs.abc.es/weblog/public/post/8-recomendaciones-para-evitar-correr-riesgos-en-redes-sociales-14100.asp/